CLAIMS

Having thus described our invention, what we claim as new and desire to secure by Letters Patent is as follows:

1. A method of protecting a document which will be transformed into a value bearing instrument after adding additional markings to the document from fraudulent alteration of the markings comprising the steps of:

generating encryptions of a unique identifier X of the document, the unique identifier X being printed on the document; and

covering each critical field k, k=1,2,3..., of the document where markings are to be added with encrypted versions of X, $\mathrm{Sign}_{k,0}(X)$, where $\mathrm{Sign}_{k,0}(X)$ is a cryptographic function or family thereof which is known only to an institution which issues the document, $\mathrm{Sign}_{k,0}(X)$ being used to authenticate the document.

2. The method of protecting a document from fraudulent alteration recited in claim 1, wherein an entire area of a field k is covered with a large number of lines of fine print, the lines of fine print comprising one of several encryptions of X.

3. The method of protecting a document from fraudulent alteration recited in claim 2, wherein each critical field k of the document, in addition to being covered by the encrypted version of X, $\mathrm{Sign}_{k,0}(X)$, is covered with another encrypted version of X, $\mathrm{Sign}_k(X)$, where $\mathrm{Sign}_k(X)$ is another cryptographic function or family thereof different from the cryptographic function $\mathrm{Sign}_{k,0}(X)$ which is known to a larger number of authorized institutions for performing an initial authentication of the document.

4. The method of protecting a document from fraudulent alteration recited in claim 2, wherein each critical field k of the document, in addition to being covered by the encrypted version of X, $\mathrm{Sign}_{k,0}(X)$, is covered with another encrypted version of X, $\mathrm{Sec}_k(X)$, where $\mathrm{Sec}_k(X)$ is another cryptographic function or family thereof different from the cryptographic function $\mathrm{Sign}_{k,0}(X)$ which is known to a small group within the institution which issues the document for performing final authentication of the document

5. The method of protecting a document from fraudulent alteration recited in claim 3, wherein each critical field k of the document, in addition to being covered by encrypted versions of X, $\mathrm{Sign}_k(X)$ and $\mathrm{Sign}_{k,0}(X)$, is covered with a third encrypted version of X, $\mathrm{Sec}_k(X)$, where $\mathrm{Sec}_k(X)$ is another cryptographic function or family thereof different from the cryptographic functions $\mathrm{Sign}_{k,0}(X)$ and $\mathrm{Sign}_k(X)$ which is known to a small group within the institution which issues the document for performing final authentication of the document

6. The method of protecting a document from fraudulent alteration recited in claim 5, further comprising the step of indexing the cryptographic functions Sign_k, $\mathrm{Sign}_{k,0}$ and Sec_k, by a number corresponding to the field k, so that each line comprises different encryptions of X such that each cryptographic function $\mathrm{Sign}_k(X)$, $\mathrm{Sign}_{k,0}(X)$ and $\mathrm{Sec}_k(X)$ is a family of different cryptographic functions.

7. The method of protecting a document from fraudulent alteration recited in claim 6, wherein the families of cryptographic functions Sign_k, $\mathrm{Sign}_{k,0}$ and Sec_k prevent cryptographic functions which have been obscured at different

places by marks added to the document from being used to reconstitute the full cryptographic function.

8. The method of protecting a document from fraudulent alteration recited in claim 1, wherein electronic deposit of a document transformed into a value bearing instrument comprises the steps of:

scanning the document with a scanner to generate a digitized version of the document; and

transmitting the digitized version of the document for deposit.

9. The method of protecting a document from fraudulent alteration recited in claim 8, wherein electronic deposit of a document transformed into a value bearing instrument further comprises the step of endorsing the document, if needed, having printed thereon encryptions in at least selected locations where markings are added to transform the document into a value bearing instrument, the act of endorsing obscuring some of the encryptions.

10. The method of protecting a document from fraudulent alteration recited in claim 8, wherein electronic deposit of a document transformed into a value bearing instrument further comprises the steps of:

extracting from the digitized version of the document the unique identifier X and a corresponding digital encryption of X, $\text{Sign}_k(X)$, which is known to a large number of authorized institutions; and

comparing a decrypted version of $\text{Sign}_k(X)$ to the unique identifier X as an initial authentication of the document.

11. The method of protecting a document from fraudulent alteration recited in claim 10, wherein electronic deposit of a document transformed into a value

bearing instrument further comprises the steps of:

extracting from the digitized version of the document the unique identifier X and a corresponding digital encryption of X, $\mathrm{Sign}_{k,0}(X)$, which is known only to an institution that issues the document; and

comparing a decrypted version of $\mathrm{Sign}_{k,0}(X)$ to the unique identifier X as a further authentication of the document.

12. The method of protecting a document from fraudulent alteration recited in claim 11, wherein electronic deposit of a document transformed into a value bearing instrument further comprises the steps of:

extracting from the digitized version of the document the unique identifier X and a corresponding digital encryption of X, $\mathrm{Sec}_k(X)$, which is known to a small group within the institution that issues the document; and

comparing a decrypted version of $\mathrm{Sec}_k(X)$ to the unique identifier X as a final authentication of the document.

13. The method of protecting a document from fraudulent alteration recited in claim 1, wherein portions of the lines of fine print are obscured by writing added to the document when transforming the document into a value bearing instrument.

14. The method of protecting a document from fraudulent alteration recited in claim 13, wherein the document is a check and the unique identifier X is check data comprising a bank Id number, an account Id number and a check number.

15. The method of protecting a document from fraudulent alteration recited in claim 14, wherein an issuing bank chooses a first secret key Sign_k using a

secure cryptographic generator (SCG), further comprising the steps of:

computing a first family of encrypted functions $\mathrm{Sign}_k(X)$; and

communicating the key Sign_k to banks and other authorized institutions involved in depositing of checks, the family of encrypted functions $\mathrm{Sign}_k(X)$ allowing the payee's bank to perform a first authentication of the check.

16. The method of protecting a document from fraudulent alteration recited in claim 15, wherein an issuing bank chooses a second secret key $\mathrm{Sign}_{k,0}$ using a SCG, further comprising the steps of:

computing a second family of encrypted functions $\mathrm{Sign}_{k,0}(X)$, key $\mathrm{Sign}_{k,0}$ remaining the exclusive property of the issuing bank; and

using SCGs, communicating the key $\mathrm{Sign}_{k,0}$ to all branches of the issuing bank where check clearing is done, the family of encrypted functions $\mathrm{Sign}_{k,0}(X)$ being used exclusively by the issuing bank and branches involved in the clearing of checks.

17. The method of protecting a document from fraudulent alteration recited in claim 16, wherein an issuing bank chooses a third secret key Sec_k which is exclusively known to a small group within the issuing bank, further comprising the step of computing a third family of encrypted functions $\mathrm{Sec}_k(X)$, the secret key Sec_k being used by the issuing bank as final instrument to verify the check.

18. The method of protecting a document from fraudulent alteration recited in claim 14, wherein the check is deposited by a payee electronically from a location remote from a bank or Automatic Teller Machine (ATM) .

19. The method of protecting a document from fraudulent alteration recited in

claim 14, wherein electronic deposit of the check by a payee comprises the steps of:

endorsing the check having printed thereon encryptions in at least selected locations where information is written by a payer, the act of endorsing by the payee obscuring some of the encryptions;

scanning the endorsed check with a scanner to generate a digitized version of the check;

transmitting the digitized version of the check for deposit to the payee's bank.

20. The method of protecting a document from fraudulent alteration recited in claim 19, wherein electronic deposit of the check by a payee comprises the steps of:

extracting by the payee's bank from the digitized version of the check the unique identifier X and a corresponding digital encryption of X, $\mathrm{Sign}_k(X)$, which is known to a large number of authorized institutions including the payee's bank; and

comparing by the payee's bank a decrypted version of $\mathrm{Sign}_k(X)$ to the unique identifier X as an initial authentication of the check.

21. The method of protecting a document from fraudulent alteration recited in claim 20, wherein electronic deposit of the check further comprises the steps of:

extracting from the digitized version of the check the unique identifier X and a corresponding digital encryption of X, $\mathrm{Sign}_{k,0}(X)$, which is known only to a bank that issues the check; and

comparing by the payor's bank a decrypted version of $\mathrm{Sign}_{k,0}(X)$ to the unique identifier X as a further authentication of the check.

22. The method of protecting a document from fraudulent alteration recited in claim 21, wherein electronic deposit of the check further comprises the steps of:

extracting from the digitized version of the check the unique identifier X and a corresponding digital encryption of X, $\mathrm{Sec}_k(X)$, which is known to a small group within the bank that issues the check; and

comparing a decrypted version of $\mathrm{Sec}_k(X)$ to the unique identifier X as a final authentication of the check.

23. The method of protecting a document from fraudulent alteration recited in claim 19, further comprising the step of accessing a database by the payee's bank where the unique identifier X and first encrypted function $\mathrm{Sign}_k(X)$ is registered to determine whether the check has been previously presented for deposit.

24. The method of protecting a document from fraudulent alteration recited in claim 19, further comprising the step of registering a check to be deposited by the payee with an SCG to prevent multiple deposits.

25. A document protecting against fraudulent alteration of markings added to the document to transform the document into a value bearing instrument, the document having printed thereon and covering each critical field k, k=1,2,3..., where markings are added to the document encrypted versions a unique identifier X printed on the document, $\mathrm{Sign}_{k0}(X)$, where $\mathrm{Sign}_{k0}(X)$ is a cryptographic function or family thereof which is known only to an institution which issues the document, $\mathrm{Sign}_{k0}(X)$ being used to authenticate the document.

26. The document recited in claim 25, wherein an entire area of field k is covered with a large number of lines of fine print, the lines of fine print comprising an encryption of X.

27. The document recited in claim 26, wherein each critical field k of the document, in addition to being covered by encrypted versions of X, $\mathrm{Sign}_{k0}(X)$, is covered with another encrypted version of X, $\mathrm{Sign}_{k}(X)$, where $\mathrm{Sign}_{k}(X)$ is another cryptographic function or family thereof different from the cryptographic function $\mathrm{Sign}_{k,0}(X)$ which is known to a larger number of authorized institutions for performing an initial authentication of the document.

28. The document recited in claim 27, wherein each critical field k of the document, in addition to being covered by encrypted versions of X, $\mathrm{Sign}_{k,0}(X)$ and $\mathrm{Sign}_{k}(X)$, is covered with a third encrypted version of X, $\mathrm{Sec}_{k}(X)$ is another cryptographic function or family thereof different from the cryptographic functions $\mathrm{Sign}_{k,0}(X)$ and $\mathrm{Sign}_{k}(X)$ which is known to a small group within the institution which issues the document for performing final authentication of the document.

29. The document recited in claim 28, wherein the cryptographic functions Sign_{k}, $\mathrm{Sign}_{k,0}$ and Sec_{k}, are indexed by a number corresponding to the field k, so that each line comprises different encryptions of X such that each cryptographic function $\mathrm{Sign}_{k}(X)$, $\mathrm{Sign}_{k,0}(X)$, $\mathrm{Sec}_{k}(X)$ is a family of different cryptographic functions.

30. The document recited in claim 29, wherein the act of adding markings to

the document to transform the document into a value bearing instrument obscures some of the encryptions, the families of different cryptographic functions preventing cryptographic functions which have been obscured at different places from being used to reconstitute the full cryptographic function.

31. The document recited in claim 25, wherein the document is a check and the unique identifier X is check data comprising a bank Id number, an account Id number and a check number.

32. The document recited in claim 31, wherein the act of adding markings to the check to transform the document into a value bearing instrument obscures some of the encryptions

33. The document recited in claim 32, wherein an entire area of field k is covered with a large number of lines of fine print, the lines of fine print comprising an encryption of X.

34. The document recited in claim 33, wherein each critical field k of the document, in addition to being covered by encrypted versions of X, $\mathrm{Sign}_{k0}(X)$, is covered with another encrypted version of X, $\mathrm{Sign}_{k}(X)$, where $\mathrm{Sign}_{k}(X)$ is another cryptographic function or family thereof different from the cryptographic function $\mathrm{Sign}_{k,0}(X)$ which is known to a larger number of authorized banks and institutions for performing an initial authentication of the check.

35. The document recited in claim 34, wherein each critical field k of the document, in addition to being covered by encrypted versions of X, $\mathrm{Sign}_{k,0}(X)$

and $\mathrm{Sign}_k(X)$, is covered with a third encrypted version of X, $\mathrm{Sec}_k(X)$ is another cryptographic function or family thereof different from the cryptographic functions $\mathrm{Sign}_{k,0}(X)$ and $\mathrm{Sign}_k(X)$ which is known to a small group within the bank or institution which issues the check for performing final authentication of the check.

36. The document recited in claim 35, wherein the encrypted function $\mathrm{Sign}_k(X)$ are communicated to banks and other authorized institutions involved in depositing checks and the encrypted function $\mathrm{Sign}_k(X)$ allows the payee's bank to perform a first authentication of the check.

37. The document recited in claim 36, wherein key $\mathrm{Sign}_{k,0}$ remains the exclusive property of the issuing bank and the encrypted function $\mathrm{Sign}_{k,0}(X)$ is used exclusively by the issuing bank and branches involved in the clearing of checks.

38. The document recited in claim 37, wherein secret key Sec_k is exclusively known to the issuing bank and the encrypted function $\mathrm{Sec}_k(X)$ is used by the issuing bank as a final instrument to verify the check.